schwarz digits

Service certificate

STACKIT Secrets Manager

Version and start of validity	
Version 1.4	Valid from 2025/09/12

Service certificate | STACKIT Secrets Manager

Service name

STACKIT Secrets Manager

High level service description

STACKIT Secrets Manager (“Secrets Manager”) is a managed service that provides a secure key-value store for sensitive data (such as passwords, configuration files and text). It enables the protection and management of secrets. The Secrets Manager provides an API that enables easy integration into applications and workflows. This allows the separation of source code and secrets, and compliance requirements can be implemented.

Key features

- Storage of secrets according to security requirements (e.g., separation of source code andsecrets)
- The customer can order a Secrets Manager fast and simply using the self-service user interface in the STACKIT Portal
- Secrets can be managed via a user-friendly configuration interface and API
- Traceability of changes through versioning of individual secrets
- High availability guarantees the safe operation of the Secrets Manager
- Pre-configured auto-update functions keep components up-to-date

Service plans

The Secrets Manager automatically scales in the number of secrets, secret versions and users.

The following limitations apply:

- the number of API accesses per Secrets Manager is limited to 10,000 accesses per hour
- up to 100 users can be created per Secrets Manager

up to 1 MB of text can be stored in the form of key-value pairs for each secret version

Metrics

- Billing takes place by the hour according to the number of secret versions.

SLA specifics

- Secrets Manager is considered available as long as the API and configuration interface are accessible at the service delivery point.

Backup

- There is no customer-specific backup. The Secrets Manager automatically saves a preconfigured number of secret versions (unlimited by default). If a version limit is set and exceeded the oldest versions will be deleted.

Additional terms

- The customer is responsible for the configuration of Secrets Manager (in particular the management of accounts and version limit).

Annex | Exportability

(Online Register)

Data type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data (database content)	Data stored by the customer in the database (if available) or within the product/service	Yes	JSON	Data export is possible via the Hashicorp compatible API
User accounts & permissions	Information about users and their permissions	Yes	JSON	The password can not be exported
System metrics (instances / resources in use)	Performance data of the instance / resource in use (e.g., CPU usage, memory usage)	No. Company confidential STACKIT.		
	Sizes and capacities *Capacities of the available resources / instances*	Yes	JSON	Amount of Secrets and Versions
System properties (instances / resources in use)	Versions and information necessary to check compatibility	No. Company confidential STACKIT.	-	-
Product / service-related data (product properties)	Configuration data and source code *Configuration of IT-systems / rudimental IT, settings, customizing, IP's, VLAN, interfaces, software code, scripts*	No. Company confidential STACKIT.	-	-
	Log data (non personalized and personalized) *System-status, technical-events, etc.*	No. Company confidential STACKIT.	-	-

Log data (non personalized and personalized) *Login/logout of user, user activities*	Yes	JSON	Events can be exported via the STACKIT Auditlog API